Serial No. 09/503,122
WH-10 752US

Remarks

Attached hereto is a marked version of the claims showing additions and deletions.

We enclose for the Examiner's review and consideration, certain pages from Nex Flash Technologies Inc. describing and/or referring to Serial Flash Memory devices. It is submitted this term is well known to a person skilled in this art and the application and claims fully comply with Section 112, first and second paragraphs. Reconsideration and withdrawal of this rejection is requested.

The present invention is directed to a banknote validator which can be conveniently updated in the field, as may be required, perhaps several years after the original sale of the validator. The prior art reference of Mazur et al. as well as the background of the present application, outline why such a banknote validator would require updating, including the issuance of new banknotes by a government, the updating of the evaluation process to recognize certain fraudulent banknotes, or perhaps to allow the validator to evaluate banknotes of a different country.

The purpose of a banknote validator is to recognize fraudulent banknotes which is difficult due to the increasing sophistication of the fraudulent activities. Better paper, more accurate copying and improved colour control makes the detection of fraudulent bills difficult.

Validators are designed to evaluate the banknotes and make an informed decision in a relatively short period of time as the customer is completing an automated purchase. To improve the reliability of the validator, it has been recognized that the information used by the validator to evaluate the banknote, may require updating from time to time. Mazur et al. states that

this updating of validators has been carried out in the past by returning the validator to a service depot or having a skilled technician reprogram the validator.

Each of these processes worked satisfactorily, however, there is a relatively high cost associated with the updating process. To overcome this problem, the Mazur et al. structure designs a validator which can be set in a "learn mode", and specialized master banknotes are scanned by the validator to reprogram the device. It is further fundamental to the structure that this master information may be copied from the memory of a primary machine to the memory of one or more secondary machines, as described in column 36, lines 33 through 55. Unfortunately, the method of updating a currency validator as set out in the Mazur et al. patent, has a number of serious security disadvantages. These disadvantages are further compounded by the lack of control in updating currency validators that are often used in stand alone vending machines, gaming machines and other applications. Furthermore, each of the validators, as taught by Mazur et al. must operate in several different modes and this capability further adds to the cost of the validator.

As any of these machines can essentially be reprogrammed according to Mazur, by merely placing the validator in a learn mode, and feeding master documents to the validator, they are subject to a fraudulent activity. For example, a service technician could substitute master banknotes which have been specifically designed to accept certain fraudulent bills. Furthermore, this type of system also provides or has the potential to provide, information to counterfeiters which will allow them to improve the counterfeit quality, such that the fraudulent banknotes are accepted by an updated validator. If these master documents fall into the wrong hands, the counterfeiters know the precise standard for evaluating

banknotes. In this way, the counterfeit bills can be optimized to be accepted. This is a serious disadvantage, particularly, in light of the number of master documents that must be available to different users to update their particular validators. Furthermore, it can be appreciated that the master documents provided to one operator are typically the same master documents that would be provided to other operators.

The updating of a currency validator in the field by the operator or an unskilled repair person is desirable from a cost point standpoint, but exposes the validator to a further security attack. The present invention, as defined by the claims of the application address this issue while still providing a high degree of security against fraudulent reprogramming of the validator and without providing the standard for evaluating banknotes.

The claims of the present application require a banknote validator which is designed to receive a removable memory storage arrangement and the central processing unit of the validator includes a testing procedure of any received removable storage arrangement, inserted in the device. The central processing unit only downloads information from the received removable storage arrangement, which modifies the operation of the validator upon positive evaluation of the integrity of the removable memory storage arrangement. The integrity of the removable memory storage arrangement has been determined by using the testing procedure of the central processing unit.

The process as described in the preferred embodiment of the invention includes encryption of the removable memory storage arrangement where personal information of the memory storage arrangement is also encrypted together with the new processing information which will eventually be downloaded. The central

processing unit can then use the test procedure to evaluate the integrity of the memory storage arrangement, preferably by determining whether the serial number provided with the removable memory storage arrangement matches with the serial number which has been encrypted. If the information has been tampered with, this can typically be detected in that the serial number will not match. Furthermore, the exact location of the encrypted serial number will not be known to any counterfeiters. With this security arrangement built into the validator at its time of manufacture, the validator can then be updated in the field basically securely, while still providing the advantages of low cost installation as no high degree of training is required. Security is essentially maintained by the manufacturer. The memory stick is not particularly helpful to a counterfeiter as the information has been encrypted.

In a preferred embodiment of the invention, any validator which has been updated requires the removable memory arrangement to be maintained in the validator for operation of the validator. In this way, the removable memory arrangement becomes part of the operating validator and is not a disposable device. This again reduces the possibility of the memory arrangements being easily available for possible counterfeiting activities.

In yet a further aspect of the invention, the removable memory arrangement initially provides information used by the central processing unit to evaluate banknotes and thereafter provides additional memory for the processing of the banknotes during normal operation of the validator.

As acknowledged in the Official Action, the primary reference does not include any security features as required by the present claims. Hardy et al. discloses a secure process

where documents can be exchanged over a computer network by using
" digital signatures". This digital signature process is a very
secure process requiring a private key, a public key and what is
referred to as a "K" key.

        In column 9 of the patent, a non-volatile memory 122
such as a flash memory card, is used to durably and securely
store a user's private key 124 or the internal "K" key, state
value 126. Thus the important security keys are stored in a
removable flash memory card. It is stated that the values stored
in the non-volatile memory may be encrypted using a password or
PIN value as the encryption key. There is no teaching of using a
removable memory storage device which has a readily available
serial number for example, that is also encrypted with other
information to be downloaded to a validator for updating of the
validator. Furthermore, there is no teaching of a validator with
a central processing unit which includes a testing procedure for
a evaluating the encrypted information and determining the
authenticity thereof based on this information. Note that the
arrangement disclosed in the Hardy patent requires other
information such as a PIN number or password. This arrangement
is not the same as proposed in the present application and if the
references were combined, they would not operate in the manner of
the claimed invention.

        The Official Action further argues that these references
are analogous art as they both concern the use of flash memory
cards. This position is respectfully traversed. It is noted
that the international class, the U.S. classes as well as the
related additional classes used to classify the references do not
overlap. Furthermore, the primary reference is directed to
banknote validators and the operation of banknote validators.
The secondary reference is concerned with the exchange of
financial documents between computer systems typically over a

public network. There is a requirement for these computer systems to have documentation which cannot be refuted. The particular process described in this patent requires extensive computer capabilities which are not typically available in a stand alone validator. Furthermore, there is nothing in the primary reference or the secondary reference which would suggest these references should be combined. In particular, the primary reference which includes some 49 columns of description and various alternate structures for carrying out the invention, failed to disclose any mention of security features which can be accomplished by means of encryption of a flash card.

Furthermore, the primary reference essentially teaches away from the concept of the present invention where control is maintained by the manufacturer and the manufacturer produces removable memory storage arrangements which can be used by earlier sold validators which have a built in test procedure. In the present invention, the validator must make its own determination as it is typically a stand alone unit. The security check is carried out by the validator. This is in contrast to the secondary reference which requires the exchange of documents and the exchange of keys used as part of the encryption process.

The secondary reference with respect to the flash memory card clearly teaches the encryption of certain key information using a PIN or password which is only available to the operator. In the case of updating a validator, a relatively unskilled technician would be required to know the password resulting in a further security risk. Therefore the security features of the secondary reference are in contradiction to the automated test evaluation defined in the present claims.
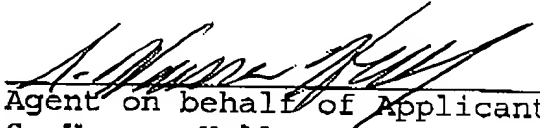
Serial No. 09/503,122
WH-10 752US

In a further aspect of the invention which has been claimed in new claims 16 through 20, the validator is designed to have replaceable sensors and a validator may be updated by updating of the sensors as well as the updating of the software used for the evaluation of the banknotes. In this way, the type of sensors, as well as the location of the sensors, and the part of the banknote being evaluated, can be changed from time to time and provides the manufacturer with additional flexibility with respect to the effective updating of validators that have been previously sold.

In view of the above, reconsideration and allowance of the application is requested.

Respectfully submitted,

Agent on behalf of Applicant
S. Warren Hall
Registration No. 30,350
(416) 368-8313

WH/sdw
Encl.

VERSION WITH MARKINGS TO SHOW CHANGES

Claims 7 and 9 have been cancelled.

The remaining claims have been amended as follows:

1.   A banknote validator comprising a banknote processing channel, a series of sensors located along said channel for scanning a banknote as it moves past said sensors, a central processing unit for controlling the operation of said validator and receiving and processing the signals from said sensors, and a removable memory storage arrangement insertable in a receiving location of said validator, said removable memory storage arrangement when received in said receiving location forming an electrical communication path with said central processing unit, said central processing unit including a testing procedure which evaluates the integrity of any received removable memory storage arrangement and said central processing unit downloading information from said received removable storage arrangement for operation thereof upon positive evaluation of the integrity of said removable memory storage arrangement. providing thereto logic for operating said validator.

2.   A banknote validator as claimed in claim 1 wherein said removable memory storage arrangement is a serial flash memory module.

3.   A banknote validator as claimed in claim 1 wherein the removable memory storage arrangement includes an electronic address available to the central processing unit and the electronic address is used to confirm the encoded software remains unchanged as part of said testing procedure.

4.   A banknote validator as claimed in claim 1 2 wherein the serial flash module contains information to be downloaded to the central processing unit for controlling the operation of the validator and said central processing unit of the validator will not allow the validator to operate if the central processing unit has previously downloaded information from a serial flash memory module and a serial flash memory module is not inserted therein received in said validator.

5.   A banknote validator as claimed in claim 3 wherein the removable flash memory module contains encrypted algorithms used by the central processing unit to evaluate banknotes for authenticity and the central processing unit includes decryption software

for decoding the algorithms and storing the decoded algorithms in said central processing unit.

6.   A serial flash memory module for updating a validator comprising a read only memory which includes an identification code specific to the serial flash memory module and a rewritable memory containing encrypted operating software for operating a validator, said encrypted software including encryption of at least part of said identification code.

8.   A banknote validator as claimed in claim 7 3 wherein said removable memory storage arrangement provides additional memory available to said central processing unit for evaluation of banknotes.

12.   A banknote validator as claimed in claim 2 wherein said serial flash memory module contains information to be downloaded to said central processing unit for controlling the operation of said validator, said serial flash module after downloading of said information including a security feature such that said serial flash module can not be used with other validators.

13.   A banknote validator as claimed in claim 11 wherein said serial flash memory module records the electronic address of the validator when received in said receiving arrangement and only communicates with said central processing unit when there is a match between the recorded electronic address and the electronic address provided by the validator.

14.   A banknote validator as claimed in claim 1 wherein said removable memory storage arrangement provides additional memory available to said central processing unit for evaluation of banknotes.

15.   A banknote validator as claimed in claim 1 2 wherein said removable memory storage arrangement contains encrypted algorithms used by the central processing unit to evaluate banknotes for authenticity.
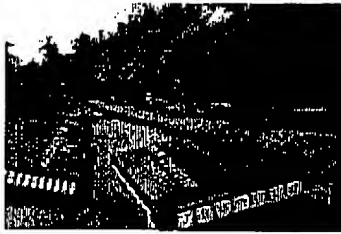
NexFlash Technologies, Inc.

COMPANY

- About
- Press Releases
- Employment
- Directions Map

PRODUCTS

- Product Selector Guide
- Serial Flash
- Parallel Flash
- Presentations
- Company &
  Product Photos

SALES

- International
- North American
- Online Store

CONTACT

- Sales @ NexFlash
- Webmaster

To view the Data Sheets on this site,
download a free version of Acrobat
Reader

Get Acrobat

NexFlash Overview

NexFlash Technologies, Inc. designs and markets Specialty Flash Memory Products for today's emerging applications. Product lines include High-Speed Parallel Flash and Low-Power Serial Flash Memories and Modules. NexFlash holds numerous patents on its technology and has strategic alliances and partnerships with Winbond Electronics, Sharp Corp., ISSI, Chartered Semiconductor and UMC. **More**

Click above for more information.

Learn More About NexFlash
New HTML Slide Shows on NexFlash products and applications

Worlds Fastest 1M-bit Flash!
The NX29F010 is fast, drop-in compatible, and available in a variety of packages and temperature grades.

Flash Memory without the Baggage
Serial Flash Memories and Modules use less power, space, and fewer pins than ordinary Flash. Tell me more!

Serial Flash Development Kit Users!
Version 2.0 software is now available FREE UPDATE.

Upgrade Your Browser HERE!
This site is best viewed in Netscape 3.0 or higher, and Internet Explorer 4.0 or higher. NOTE: This site may not display properly in Netscape 6.0. Use the links below to get the latest version of Microsoft's Internet Explorer

NexFlash News.

HIGH-SPEED 1M-BIT (128Kx8) FLASH MEMORY

Chartered Semiconductor and NexFlash Extend Collaboration on

Embedded Flash Memory

New Product Info.

July 2001
Product Selector Guide
PDF Format

NX25F011B 1Mbit SPI Serial Flash

NX25F640 64Mbit SPI Serial Flash
PDF Format

Digital Camera Users, Got Film?

NexFLASH
Technologies, Inc.

HOME ABOUT PRODUCTS SALES EMPLOYMENT CONTACT

Serial Flash

Serial Flash Products

NexFlash's Serial Flash Memories and removable Modules offer an attractive alternative to ordinary Flash. They are ideal for applications that require data, voice and image storage, especially those constrained by power, available pins, space, performance, or other system resources. Serial Flash products are suitable for a variety of applications including portable/mobile products and microcontroller-based systems.

- **Serial Flash Overview**

- **Serial Flash Memory Data Sheets**

- **Serial Flash Module Data Sheets**

- **Application Notes**

- **Serial Flash Development Tools**

- **Accessories**

- **Technical Support**

To view the Data Sheets on this site, download a free version of Acrobat Reader

Get Acrobat

Important Update, August 2001

New "B" and "C" series Serial Flash
NexFlash's Serial Flash product line is transitioning to the new "B" and "C" series. Most "B" series devices were designed to be pin-out and function compatible with the "A" series with a few exceptions as listed below:

Key Differences of the "B" series Serial Flash:

1. The NX25F011B, NX25F021B, NX25F041B and NX25F081B devices have a single SRAM buffer instead of a dual SRAM buffer found in the "A" series. All have 264 byte sector size.

2. The NX25F011B and NX25F021B are packaged in a 28-pin TSOP1 (V) package or an 8-pin SOIC (S) package. The NX25F041B and NX25F081B are packaged in a 28-pin TSOP1 (V) package or a 28-pin SOIC (J) package.

Please note
The "A" series devices are no longer available, with the exception of the NX26F160. The latest schedule for "B" and "C" series engineering samples and production is listed below.

Data Sheet Update
If you are designing with the NX25F011/021/041B Serial Flash memory please see the latest data sheet and update notes below.

Schedule Updated as of 10/01/2001

Part Number	Data Sheets	Samples	Production	Density
NX25F011B NX26F011B	NOW Oct	NOW	NOW	1M-bit
NX25F021B NX26F021B	NOW Oct	Q1-02	Q2-02	2M-bit
NX25F041B NX26F041B	NOW Oct	Aug	Oct	4M-bit
NX25F081B		*	*	

NX26F081B	NexFlash			NexFlash	
NX25F080C NX26F080C	NexFlash*			NexFlash*	
NX25F160C NX26F160C	Oct Oct	Q1-02		Q2-02	16M-bit
NX25F320C NX26F320C	Q4-01	Q2-02		Q3-02	32M-bit
NX25F640C NX26F640C	Advanced	Q4-01		Q1-02	64M-bit

*
Contact NexFlash Marketing for the latest
information on this product.
sales@nexflash.com

Serial Flash Memories

Serial Interface Flash (1-Mbit to 64-Mbit) 4-pin SPI-bus, 2-Pin NXS-bus,
On-chip SRAM, Ultra-low Power, SFK Development Kit.

Size	Part No. /Data Sheet	Pkgs. Available	Comments
1-Mbit 4-pin SPI	NX25F011A-3V-R NX25F011A-5V-R LAST UPDATED 06/11/99	TSOP(I) "	USE NX25F011B
1-Mbit 4-pin SPI	NX25F011B-3V NX25F011B-3S NX25F011B-5V NX25F011B-5S LAST UPDATED 07/17/01	TSOP(I) SOIC "	2.7-3.6V, Icc=4 mA, Stby=1 μA 5V, Icc=8 mA, Stby=1 μA Important Data Sheet Update
1-Mbit 2-pin NXS	NX26F011A-3V (-R) NX26F011A-5V (-R) LAST UPDATED 05/05/99	TSOP(I) "	Note: The NX26F011B is function compatible with the NX26F011A
2-Mbit 4-pin SPI	NX25F021B-3V NX25F021B-3S NX25F021B-5V NX25F021B-5S LAST UPDATED 07/17/01	TSOP(I) SOIC "	2.7-3.6V, Icc=4 mA, Stby=1 μA 5V, Icc=8 mA, Stby=1 μA Important Data Sheet Update

VERSION WITH MARKINGS TO SHOW CHANGES